

Konfigurieren von IGMP-Snooping auf Switches der Serie CBS 220

Ziel

In diesem Dokument wird erläutert, wie Sie IGMP-Snooping (Internet Group Management Protocol) für die Cisco Switches der Serie Business 220 konfigurieren.

Unterstützte Geräte | Softwareversion

- Serie CBS 220 ([Datenblatt](#)) | 2,0 0,17

Einführung

Multicast ist die Technik der Netzwerkschicht, die zum Übertragen von Datenpaketen von einem Host an ausgewählte Hosts im Netzwerk verwendet wird. Auf der unteren Ebene sendet der Switch den Multicast-Datenverkehr an allen Ports, selbst wenn nur ein Host diesen empfangen muss. Internet Group Management Protocol (IGMP)-Snooping wird verwendet, um IPv4-Multicast-Datenverkehr (Internet Protocol Version 4) an den gewünschten Host weiterzuleiten.

Wenn IGMP aktiviert ist, werden die IGMP-Nachrichten erkannt, die zwischen dem IPv4-Router und den an die Schnittstellen angeschlossenen Multicast-Hosts ausgetauscht werden. Anschließend wird eine Tabelle verwaltet, die den IPv4-Multicast-Datenverkehr beschränkt und dynamisch an die Teile weiterleitet, die diese Daten empfangen müssen.

Die folgenden Konfigurationen sind Voraussetzung für die IGMP-Konfiguration:

- [Virtual Local Area Network \(VLAN\) konfigurieren](#)
- Bridge-Multicast-Filterung aktivieren (Schritte im nächsten Abschnitt dargestellt)

IGMP-Snooping und Multicast-Aktion aktivieren

Damit IGMP-Snooping funktioniert, muss die Bridge-Multicast-Filterung aktiviert werden. IGMP-Snooping muss global und für jedes relevante VLAN auf der IGMP-Snooping-Seite aktiviert werden.

Schritt 1

Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Multicast > Properties** aus.

1 Multicast

2 Properties

Schritt 2

Stellen Sie sicher, dass IGMP-Snooping aktiviert ist. Wählen Sie die Prozedur für *Unbekannte Multicast-Aktion* aus. Die Optionen sind *Drop*, *Flood* oder *Forward to Router Port*.

Properties

IGMP Snooping: Enable

MLD Snooping: Enable

Unknown Multicast Action: Drop
 Flood
 Forward to Router Port

Schritt 3

Klicken Sie auf Apply (Anwenden).

Konfigurieren von IGMP-Snooping

Schritt 1

Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Multicast > IGMP Snooping** aus.



Schritt 2

Wählen Sie das Optionsfeld für die IGMP-Version aus, die Sie verwenden möchten. Ihre Optionen sind IGMPv2 oder IGMPv3.

Die Berichtunterdrückung ist standardmäßig aktiviert. Wenn Sie diese Funktion deaktivieren, werden alle IGMP-Berichte an Multicast-Router weitergeleitet.

Die Unterdrückung von IGMP-Berichten wird nur unterstützt, wenn die Multicast-Abfrage IGMPv1- und IGMPv2-Berichte enthält. Diese Funktion wird nicht unterstützt, wenn die Abfrage IGMPv3-Berichte enthält. Der Switch verwendet die IGMP-Berichtsunterdrückung, um pro Multicast-Router-Abfrage nur einen IGMP-Bericht an Multicast-Geräte weiterzuleiten. Wenn die Unterdrückung von IGMP-Berichten aktiviert ist, sendet der Switch den ersten IGMP-Bericht aller Hosts für eine Gruppe an alle Multicast-Router. Der Switch sendet die verbleibenden IGMP-Berichte für die Gruppe nicht an die Multicast-Router. Diese Funktion verhindert, dass doppelte Berichte an die Multicast-Geräte gesendet werden. Der Switch leitet immer nur den ersten IGMPv1- oder IGMPv2-Bericht von allen Hosts für eine Gruppe an alle Multicast-Router weiter. Unabhängig von der Multicast-Router-Abfrage enthält er auch Anforderungen für IGMPv3-Berichte.

IGMP Snooping

IGMP Snooping Version: IGMPv2

IGMPv3

Report Suppression: Enable

Schritt 3

Wählen Sie ein VLAN aus, und klicken Sie auf das **Bearbeitungssymbol**.

IGMP Snooping Table



2

Entry No.	VLAN ID	IGMP Snooping Operational Status
-----------	---------	----------------------------------

<input type="radio"/>	1	1	Disabled
-----------------------	---	---	----------

1

<input checked="" type="radio"/>	2	2	Disabled
----------------------------------	---	---	----------

Schritt 4

Aktivieren Sie das Kontrollkästchen Aktivieren für *IGMP-Snooping-Status*. Dadurch wird IGMP-Snooping im VLAN aktiviert. Das Gerät überwacht den Netzwerkverkehr, um festzustellen, welche Hosts Multicast-Datenverkehr gesendet werden sollen.

VLAN ID:

2 ▾

IGMP Snooping Status:

Enable

Schritt 5 (optional)

Damit der Multicast-Router die angeschlossenen Ports automatisch erkennt, aktivieren Sie das Kontrollkästchen Enable (Aktivieren) für *MRouter Ports Auto Learn*

(Automatisch lernen).

VLAN ID: ▾

IGMP Snooping Status: Enable

MRouter Ports Auto Learn: Enable

Schritt 6

Abfragezuverlässigkeit - Geben Sie die Starkheitsvariable ein, die verwendet werden soll, wenn es sich bei diesem Switch um den ausgewählten Abfrage-Abfrager handelt.

VLAN ID: ▾

IGMP Snooping Status: Enable

MRouter Ports Auto Learn: Enable

Query Robustness: (Range: 1 - 7, Default: 2)

Schritt 7

Abfrageintervall - Geben Sie das Intervall zwischen den allgemeinen Abfragen ein, die verwendet werden sollen, wenn es sich bei diesem Schalter um den ausgewählten Abfrage-Parameter handelt.

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Schritt 8

Query Max Response Interval (Max. Antwortintervall abfragen): Geben Sie die Verzögerung ein, die zum Berechnen des maximalen Antwortcodes verwendet wird, der in die periodischen allgemeinen Abfragen eingefügt wurde.

MRouter Ports Auto Learn: Enable

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

Schritt 9

Zähler für letzte Mitgliederabfrage - Die Anzahl der gruppenspezifischen IGMP-

Abfragen, die gesendet werden, bevor das Gerät davon ausgeht, dass es keine weiteren Mitglieder für die Gruppe gibt, wenn das Gerät der gewählte Querier ist.

MRouter Ports Auto Learn: Enable

✳ Query Robustness: (Range: 1 - 7, Default: 2)

✳ Query Interval: sec (Range: 30 - 18000, Default: 125)

✳ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✳ Last Member Query Counter: (Range: 1 - 7, Default: 2)

Schritt 10

Intervall für letzte Mitgliederabfrage - Geben Sie die maximale Antwortzeit ein, die verwendet werden soll, wenn der Switch den maximalen Wert für die Antwortzeit aus gruppenspezifischen Abfragen nicht lesen kann, die vom ausgewählten Abfrage gesendet wurden.

MRouter Ports Auto Learn: Enable

✳ Query Robustness: (Range: 1 - 7, Default: 2)

✳ Query Interval: sec (Range: 30 - 18000, Default: 125)

✳ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✳ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✳ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Schritt 11

Sofort verlassen: Wählen Sie diese Option aus, damit der Switch eine Schnittstelle entfernen kann, die eine Urlaubsmeldung aus der Weiterleitungstabelle sendet, ohne zuvor MAC-basierte allgemeine Abfragen an die Schnittstelle zu senden. Wenn eine IGMP-Leave-Nachricht von einem Host empfangen wird, entfernt das System den Host-Port aus dem Tabelleneintrag. Nachdem die IGMP-Abfragen vom Multicast-Router weitergeleitet wurden, werden Einträge regelmäßig gelöscht, wenn keine Berichte über die IGMP-Mitgliedschaft von den Multicast-Clients empfangen werden. Wenn diese Funktion aktiviert ist, wird die Zeit reduziert, die erforderlich ist, um unnötigen IGMP-Datenverkehr zu blockieren, der an einen Geräteport gesendet wird.

MRouter Ports Auto Learn: Enable

✱ Query Robustness: (Range: 1 - 7, Default: 2)

✱ Query Interval: sec (Range: 30 - 18000, Default: 125)

✱ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✱ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✱ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

Schritt 12 (optional)

IGMP Querier Status (IGMP-Abfragerstatus) - Wählen Sie diese Funktion aus. Diese Funktion ist erforderlich, wenn kein Multicast-Router vorhanden ist.

MRouter Ports Auto Learn: Enable

✱ Query Robustness: (Range: 1 - 7, Default: 2)

✱ Query Interval: sec (Range: 30 - 18000, Default: 125)

✱ Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

✱ Last Member Query Counter: (Range: 1 - 7, Default: 2)

✱ Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

IGMP Querier Status: Enable

Schritt 13

IGMP Querier-Version - Wählen Sie die IGMP-Version aus, die verwendet werden soll, wenn das Gerät zum ausgewählten Abfrager wird. Wählen Sie IGMPv3 aus, wenn sich im VLAN Switches und/oder Multicast-Router befinden, die die Source-Specific IP Multicast Forwarding durchführen. Wählen Sie andernfalls IGMPv2 aus.

In diesem Beispiel wird Version 2 ausgewählt. Die Mitgliedschaftsabfrage kann sowohl allgemein als auch gruppenspezifisch sein. Die allgemeine Mitgliedschaftsabfrage wird verwendet, um alle Multicast-Gruppen zu bestimmen, für die die Stationen angemeldet sind. Gruppenspezifische Mitgliedschaftsabfrage wird verwendet, um zu bestimmen, ob ein Teilnehmer für eine bestimmte Gruppe vorhanden ist.

MRouter Ports Auto Learn: Enable

Query Robustness: (Range: 1 - 7, Default: 2)

Query Interval: sec (Range: 30 - 18000, Default: 125)

Query Max Response Interval: sec (Range: 5 - 20, Default: 10)

Last Member Query Counter: (Range: 1 - 7, Default: 2)

Last Member Query Interval: sec (Range: 1 - 25, Default: 1)

Immediate Leave: Enable

IGMP Querier Status: Enable

IGMP Querier Version: IGMPv2
 IGMPv3

Schritt 14

Klicken Sie auf **Apply** (Anwenden). Die Konfigurationsdatei wird aktualisiert.

Apply

Close

Änderungen in der IGMP-Snooping-Timer-Konfiguration (einschließlich Abfragezuverlässigkeit, Abfrageintervall usw.) wirken sich nicht auf Timer aus, die bereits erstellt wurden.

Schritt 15

Um diese Konfiguration aus der aktuellen Konfiguration in der Startkonfiguration zu speichern, klicken Sie auf das **Speichersymbol** oben rechts auf dem Bildschirm.

 admin(Switch...) ▾

Fazit

So einfach ist es nun, dass Sie IGMP-Snooping konfiguriert haben.

Weitere Konfigurationen finden Sie im [Cisco Business Switches der Serie 220](#).

Weitere Artikel zu CBS 220 Switches finden Sie auf der [Support-Seite](#) der [Serie 220](#).